

# Yaohui Chen

---

Facebook  
1 Hacker Way  
Menlo Park, CA, 94025

**E-mail:** yaohway@gmail.com

---

## Education

- 2017 - 2019 **Ph.D.**, *College of Computer and Information Science*, Northeastern University, Boston, MA, Advisor: Prof. Long Lu.
- 2014 - 2017 **Ph.D.**, *Department of Computer Science*, Stony Brook University (transferred to Northeastern University), Stony Brook, NY, Advisor: Prof. Long Lu.  
GPA:3.90/4.00
- 2013 - 2013 **Exchange Student**, Polytechnic University of Catalonia, Barcelona, Spain.
- 2010 - 2014 **B.Sc.**, *Department of Computer Science*, Tongji University, Shanghai, China.

---

## Research Interests

My research interests mainly include **Bug Finding Automation, Program Analysis, Binary Exploit Mitigations, Virtualization, Operating System and Mobile Security**.

---

## Experiences

- Dec. 2019 - present **Research Scientist**, *Program Analysis Team*, Facebook.
- May. 2017 - Oct. 2019 **Research Assistant**, *RiS3 Lab*, Northeastern University.
- Sep. 2018 - Dec. 2018 **Research Intern**, *Software Analysis Team*, Google.
- June. 2018 - Aug. 2018 **Research Intern**, *System Security and Privacy Research*, Microsoft Research.
- Feb. 2018 - May. 2018 **Research Intern**, *X-Lab*, Baidu USA.
- May. 2017 - Sep. 2017 **Research Intern**, *B2B Lab*, Samsung Research America.
- May. 2016 - Sep. 2016 **Research Intern**, *B2B Lab*, Samsung Research America.
- Aug. 2014 - May. 2017 **Research Assistant**, *RiS3 Lab*, Stony Brook University.

---

## Publications

**HyperFuzzer: An Efficient Hybrid Fuzzer for Virtual CPUs**, Xinyang Ge, Ben Niu, Robert Brotzman, **Yaohui Chen**, HyungSeok Han, Patrice Godefroid, Weidong Cui, In the proceedings of the 2021 ACM Conference on Computer and Communications Security (CCS'21).

**KUBO: Precise and Scalable Detection of User-triggerable Undefined Behavior Bugs in OS Kernel**, Changming Liu, **Yaohui Chen**, Long Lu, In the proceedings of the 2021 Network and Distributed System Security Symposium (NDSS'21).

**SoK: All You Ever Wanted to Know About x86/x64 Binary Disassembly But Were Afraid to Ask**, Chengbin Pang, Ruotong Yu, **Yaohui Chen**, Eric Koskinen, Georgios Portokalidis, Bing Mao, Jun Xu, In the proceeding of the 42th IEEE Symposium on Security and Privacy (Oakland'21).

**MEUZZ: Smart Seed Scheduling for Hybrid Fuzzing**, **Yaohui Chen**, Mansour Ahmadi, Reza Mirzazade farkhani, Boyu Wang, Long Lu, In the proceeding of the 23rd International Symposium on Research in Attacks, Intrusions and Defenses (RAID'20).

**SAVIOR: Towards Bug-Driven Hybrid Testing**, **Yaohui Chen**, Peng Li, Jun Xu, Shengjian Guo, Rundong Zhou, Yulong Zhang, Taowei, Long Lu, In the proceeding of the 41th IEEE Symposium on Security and Privacy (Oakland'20).

**FUDGE: Fuzz Driver Generation at Scale**, Domagoj Babic, Stefan Bucur, **Yaohui Chen**, Franjo Ivancic, Tim King, Markus Kusano, Caroline Lemieux, Laszlo Szekeres and Wei Wang, In the proceeding of The ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering (ESEC/FSE'19), (*Best Paper Award*).

**Ptrix: Efficient Hardware-Assisted Fuzzing for COTS Binary**, **Yaohui Chen**, Dongliang Mu, Zhichuang Sun, Jun Xu, Wenguo Shen, Xinyu Xing, Long Lu, Bing Mao, In Proceedings of the 14th ACM on Asia Conference on Computer and Communications Security (AsiaCCS'19).

**Compiler-assisted Code Randomization**, Hyungjoon Koo, **Yaohui Chen**, Long Lu, Vasileios P. Kemerlis, Michalis Polychronakis, In the proceeding of the 39th IEEE Symposium on Security and Privacy (Oakland'18), (*Final list, CSAW 2018*).

**InstaGuard: Instantly Deployable Hot-patches for Vulnerable System Programs on Android**, **Yaohui Chen**, Yuping Li, Long Lu, Yueh-Hsun Lin, Hayawardh Vijayakumar, Zhi Wang, Xinming Ou, In Proceedings of the 2018 Network and Distributed System Security Symposium (NDSS'18).

**Norax: Enabling Execute-Only Memory for COTS Binaries on AArch64**, **Yaohui Chen**, Dongli Zhang, Ruowen Wang, Rui Qiao, Ahmed Azab, Long Lu, Hayawardh Vijayakumar, Wenbo Shen, In the proceeding of the 38th IEEE Symposium on Security and Privacy (Oakland'17), (*Third Place of Best Paper Award in Applied Cyber Security Research, CSAW 2017*).

**Secure Integration of Web Content and Applications on Commodity Mobile Operating Systems**, Drew Davidson, **Yaohui Chen**, Franklin George, Long Lu, Somesh Jha, In Proceedings of the 12th ACM on Asia Conference on Computer and Communications Security (AsiaCCS'17).

**Shreds: Fine-grained Execution Units with Private Memory**, **Yaohui Chen**, Sebassujeen Reymondjohnson, Zhichuang Sun, Long Lu, In the proceeding of the 37th IEEE Symposium on Security and Privacy (Oakland'16).

---

## Services

- 2020 - **ACM Transactions on Privacy and Security (TOPS)**, *Journal Reviewer*.  
Present
- 2020 - **IEEE Transactions on Dependable and Secure Computing (TDSC)**, *Journal Reviewer*.  
Present
- 2016 - **IET Information Security**, *Journal Reviewer*.  
Present
- 2020 **International Symposium on Research in Attacks, Intrusions and Defenses (RAID)**, *Program Committee*.
- 2020 **ACM Conference on Computer and Communications Security (CCS)**, *Program Committee*.

---

## Honors and Awards

- 2019 **Best Paper Award**, ACM ESEC/FSE.
- 2019 **Google Fellowship Nomination**, Northeastern University.
- 2018 **RSA Scholarship**, *RSA Conference 2018*, U.S.A.
- 2017 **Best Paper Award**, CSAW, U.S.A.
- 2014 **Chair Fellowship**, *Department of Computer Science*, Stony Brook University.
- 2013 **Exchange Student Scholarship**, *Department of Computer Science*, Tongji University.
- 2012 **Second-Class Scholarship**, *Department of Computer Science*, Tongji University.

---

## Professional Skills

- OS **Linux, Android, Windows**.
- Programming **C, C++, Java, Python, System-verilog, ARM/x86/Sparc/MIPS assembly**.
- Compiler **Clang, LLVM**.
- Misc **Kubernetes, Reverse Engineering, Program Analysis, ELF Binary Linking Loading Toolchain**.